Microcontrollers & Embedded Systems		Semester	6
Course Code	**BCO601**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	3:0:2:0	SEE Marks	50
Total Hours of Pedagogy	40 hours Theory + 8-10 Lab slots	Total Marks	100
Credits	04	Exam Hours	3
Examination nature (SEE)	Theory/practical		

Course objectives:

- Understand the architectural features and instruction set of 32 bit ARM microcontrollers.
- Apply instructions of assembly language for programming ARM.
- Interpret the basic hardware components and their selection method based on the characteristics and attributes of an embedded system.
- Explain the need of real time operating system for embedded system applications.
- Develop/test/Conduct the experiments on an ARM7TDMI/LPC2148 evaluation board using Embedded 'C' and Keil Vision tool/Compiler

Teaching-Learning Process (General Instructions)

These are sample Strategies; that teachers can use to accelerate the attainment of the various course outcomes.

1. **Lecturer methods(L) need not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.**
2. **Use of Video/Animation to explain functioning of various concepts.**
3. **Encourage collaborative (Group Learning) Learning in the class.**
4. **Demonstration of sample code using Keil software.**
5. **Show the different ways to solve the same problem with different approaches and encourage the students to come up with their own creative ways to solve them.**

MODULE-1

Microprocessors versus Microcontrollers, ARM Embedded Systems: The RISC design philosophy, The ARM Design Philosophy, Embedded System Hardware, Embedded System Software, ARM Processor Fundamentals: Registers, Current Program Status Register, Pipeline, Exceptions, Interrupts, and the Vector Table , Core Extensions.

Text book 1: Chapter 1 - 1.1 to 1.4, Chapter 2 - 2.1 to 2.5 RBT: L1, L2

MODULE-2

Introduction to the ARM Instruction Set : Data Processing Instructions , Programme Instructions, Software Interrupt Instructions, Program Status Register Instructions, Coprocessor Instructions, Loading Constants

ARM programming using Assembly language: Writing Assembly code, Profiling and cycle counting, instruction scheduling, Register Allocation, Conditional Execution, Looping Constructs.

Text book 1: Chapter 3:Sections 3.1 to 3.6 (Excluding 3.5.2), Chapter 6(Sections 6.1 to 6.6) RBT: L1, L2

MODULE-3

Embedded System Components:

Embedded Vs General computing system, History of embedded systems, Classification of Embedded systems, Major applications areas of embedded systems, purpose of embedded systems

Core of an Embedded System including all types of processor/controller, Memory, Sensors, Actuators, LED, 7 segment LED display, stepper motor, Keyboard, Push button switch.

Text book 2:Chapter 1(Sections 1.2 to 1.6),Chapter 2(Sections 2.1 to 2.3) RBT: L1, L2

MODULE-4

Embedded System Design Concepts:

Characteristics and Quality Attributes of Embedded Systems, Operational quality attributes, non-operational quality attributes, Embedded Systems-Application and Domain specific, Hardware Software Co-Design and Program Modelling.

Text book 2: Chapter-3, Chapter-4, Chapter-7 (Sections 7.1, 7.2 only), RBT: L1, L2

MODULE-5

RTOS and IDE for Embedded System Design:

Operating System basics, Types of operating systems, Task, process and threads (Only POSIX Threads with an example program), Thread preemption, Multiprocessing and Multitasking, Task Communication (without any program), Task synchronization issues – Racing and Deadlock, Concept of Binary and counting semaphores (Mutex example without any program), How to choose an RTOS, Integration and testing of Embedded hardware and firmware.

Text book 2: Chapter-10 (Sections 10.1, 10.2, 10.3, 10.4 , 10.7, 10.8.1.1, 10.8.1.2, 10.8.2.2, 10.10 only), Chapter 12, RBT: L1, L2 08

PRACTICAL COMPONENT OF IPCC

Conduct the following experiments by writing programs using ARM7TDMI/LPC2148 using an evaluation board/simulator/evaluation version of Embedded 'C' & Keil Uvision-4 tool/compiler. and the required software tool.

Sl.NO	Experiments
1	Develop a program to multiply two 16 bit binary numbers.
2	Write a program to find the sum of first 10 integer numbers.
3	Write a program to find factorial of a number.
4	Write a program to add an array of 16 bit numbers and store the 32 bit result in internal RAM
5	Write a program to find the square of a number (1 to 10) using look-up table.
6	Write a program to find the largest/smallest number in an array of 32 numbers .
7	Display “Hello World” message using Internal UART.
8	Interface a Stepper motor and rotate it in clockwise and anti-clockwise direction
9	Display the Hex digits 0 to F on a 7-segment LED interface, with an appropriate delay in between
10	Interface a 4x4 keyboard and display the key code on an LCD.

Course outcomes (Course Skill Set):

At the end of the course, the student will be able to:

- Explain the architectural features and instructions of ARM microcontroller
- Apply the knowledge gained for Programming ARM for different applications.
- Demonstrate Interfacing of external devices and I/O with ARM microcontroller.
- Interpret the basic hardware components and their selection method based on the characteristics and attributes of an embedded system.
- Develop the hardware /software co-design and firmware design approaches.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

CIE for the theory component of the IPCC (maximum marks 50)

- IPCC means practical portion integrated with the theory of the course.
- CIE marks for the theory component are **25 marks** and that for the practical component is **25 marks**.
- 25 marks for the theory component are split into **15 marks** for two Internal Assessment Tests (Two Tests, each of 15 Marks with 01-hour duration, are to be conducted) and **10 marks** for other assessment methods mentioned in 22OB4.2. The first test at the end of 40-50% coverage of the syllabus and the second test after covering 85-90% of the syllabus.
- Scaled-down marks of the sum of two tests and other assessment methods will be CIE marks for the theory component of IPCC (that is for **25 marks)**.
- The student has to secure 40% of 25 marks to qualify in the CIE of the theory component of IPCC.

CIE for the practical component of the IPCC

- **15 marks** for the conduction of the experiment and preparation of laboratory record, and **10 marks** for the test to be conducted after the completion of all the laboratory sessions.
- On completion of every experiment/program in the laboratory, the students shall be evaluated including viva-voce and marks shall be awarded on the same day.
- The CIE marks awarded in the case of the Practical component shall be based on the continuous evaluation of the laboratory report. Each experiment report can be evaluated for 10 marks. Marks of all experiments' write-ups are added and scaled down to **15 marks**.
- The laboratory test **(duration 02/03 hours)** after completion of all the experiments shall be conducted for 50 marks and scaled down to **10 marks.**
- Scaled-down marks of write-up evaluations and tests added will be CIE marks for the laboratory component of IPCC for **25 marks**.
- The student has to secure 40% of 25 marks to qualify in the CIE of the practical component of the IPCC.

SEE for IPCC

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours**)

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scoredby the student shall be proportionally scaled down to 50 Marks

The theory portion of the IPCC shall be for both CIE and SEE, whereas the practical portion will have a CIE component only. Questions mentioned in the SEE paper may include questions from the practical component.

Suggested Learning Resources:

Textbooks:

1. Andrew N Sloss, Dominic Symes and Chris Wright, ARM system developers guide, Elsevier, Morgan Kaufman publishers, 2008.

2. Shibu K V, "Introduction to Embedded Systems", Tata McGraw Hill Education, Private Limited, 2 nd Edition.

Reference Books:

1. Raghunandan..G.H, Microcontroller (ARM) and Embedded System, Cengage learning Publication,2019

2. The Insider's Guide to the ARM7 Based Microcontrollers, Hitex Ltd.,1st edition, 2005.

3. Steve Furber, ARM System-on-Chip Architecture, Second Edition, Pearson, 2015.

4. Raj Kamal, Embedded System, Tata McGraw-Hill Publishers, 2nd Edition, 2008.

Web links and Video Lectures (e-Resources):

http://www.digimat.in/nptel/courses/video/106105193/L01.html
http://www.digimat.in/nptel/courses/video/106105159/L01.html
http://www.digimat.in/nptel/courses/video/106105036/L01.html

Activity Based Learning (Suggested Activities in Class)/ Practical Based Learning

• Develop and test program using ARM7TDMI/LPC2148 [5 marks]

• Demonstration of ARM7TDMI/LPC2148 evaluation board (with an experiment) using the evaluation version of Embedded 'C' & Keil Uvision-4 tool/compiler. [5 marks]

	CRYPTOGRAPHY & NETWORK SECURITY		Semester	7
	Course Code	**BCY602**	CIE Marks	50
	Teaching Hours/Week (L:T:P: S)	4:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	50	Total Marks	100
	Credits	04	Exam Hours	3
	Examination type (SEE)	Theory		

Course objectives:

1. Understand the basics of Cryptography concepts, Security and its principle
2. To analyse different Cryptographic Algorithms
3. To illustrate public and private key cryptography
4. To understand the key distribution scenario and certification
5. To understand approaches and techniques to build protection mechanism in order to secure computer networks

Teaching-Learning Process

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.
2. Use of Video/Animation to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
5. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.
6. Introduce Topics in manifold representations.
7. Show the different ways to solve the same problem with different circuits/logic and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding
9. Use any of these methods: Chalk and board, Active Learning, Case Studies

Module-1 10 hours

A model for Network Security, Classical encryption techniques: Symmetric cipher model, Substitution ciphers-Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Hill Cipher, Polyalphabetic Ciphers, One time pad, Steganography.

Block Ciphers and Data Encryption Standards: Traditional Block Cipher structures, data Encryption Standard (DES), A DES Example, The strength of DES, Block cipher design principles.

Chapter 1: 1.8 Chapter 3: 3.1, 3.2, 3.5 Chapter 4: 4.1, 4.2, 4.3, 4.4, 4.5

Module-2 10 hours

	Pseudorandom number Generators: Linear Congruential Generators, Blum Blum Shub Generator. Public key cryptography and RSA: Principles of public key cryptosystems-Public key cryptosystems, Applications for public key cryptosystems, Requirements for public key cryptography, Public key Cryptanalysis, The RSA algorithm: Description of the Algorithm, Computational aspects, The Security of RSA. Diffie-Hellman key exchange: The Algorithm, Key exchange Protocols, Man-in-the-middle Attack, Elliptic Curve Cryptography: Analog of Diffie-Hellman key Exchange, Elliptic Curve Encryption/Decryption, Security of Elliptic Curve Cryptography. Chapter 8: 8.2 Chapter 9: 9.1, 9.2 Chapter 10: 10.1, 10.4
	Module-3 10 hours
	Applications of Cryptographic Hash functions, Two simple Hash functions, Key management and distribution: Symmetric key distribution using symmetric encryption, Symmetric key distribution using asymmetric encryption, Distribution of public keys, X.509 Certificates, Public Key Infrastructures. Chapter 11: 11.1, 11.2 Chapter 14: 14.1, 14.2, 14.3, 14.4, 14.5
	Module-4 10 hours
	User Authentication: Remote user authentication principles**,** Kerberos**,** Remote user authentication using asymmetric encryption. Web security consideration, Transport layer security. Email Threats and comprehensive email security, S/MIME, Pretty Good Privacy. Chapter 15: 15.1, 15.3, 15.4 Chapter 17: 17.1, 17.2 Chapter 19: 19.3, 19.4, 19.5
	Module-5 10 hours
	Domainkeys Identified Mail. IP Security: IP Security overview, IP Security Policy, Encapsulating Security Payload, Combining security associations, Internet key exchange. Chapter 19: 19.9 Chapter 20: 20.1, 20.2, 20.3, 20.4, 20.5

Course outcome

At the end of the course, the student will be able to :

CO1: Understand the basic concepts of Cryptography and Security aspects

CO2: Apply different Cryptographic Algorithms for different applications

CO**3:** Analyze different methods for authentication and access control.

CO4: Explain key management, key distribution and Certificates.

CO5: Explain Electronic mail and IP Security.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Books

Text Books:

William stallings, "Cryptography and Network Security", Pearson Publication, Seventh Edition.

References:

1. Keith M Martin, "Everyday Cryptography", Oxford University Press.
2. V.K Pachghare,"Cryptography and Network Security", PHI, 2nd Edition.

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Group (2 students] programming assignment to implement Cryptographic Algorithms [25 marks]

	Blockchain Technology		Semester	6
	Course Code	**BCS613A**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03
	Examination type (SEE)	Theory		

Course objectives:

- To Understand Blockchain terminologies with its applications. design
- To learn working principles of Blockchain and methodologies used in Bitcoin
- To gain knowledge on Ethereum Network, Wallets, Nodes, Smart contract & DApps
- To learn blockchain Based Application Architecture using Hyperledger and the Smart Contract Lifecycle

Teaching-Learning Process (General Instructions)

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.
2. Use of Video/Animation/Demonstration to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
5. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.
6. Use animations/videos to help the students to understand the concepts.

Module-1

Distributed systems, CAP theorem, Byzantine Generals problem, Consensus. The history of blockchain, Introduction to blockchain, Various technical definitions of blockchains, Generic elements of a blockchain, Features of a blockchain, Applications of blockchain technology, Tiers of blockchain technology, Consensus in blockchain, CAP theorem and blockchain, Benefits and limitations of blockchain.

Chapter 1

Module-2

Decentralization using blockchain, Methods of decentralization, Blockchain and full ecosystem decentralization, Smart contract, Decentralized organizations, Decentralized autonomous organizations, Decentralized autonomous corporations, Decentralized autonomous societies Decentralized applications, Platforms for decentralization.

Cryptographic primitives: Symmetric cryptography, Asymmetric cryptography, Public and private keys, Hash functions: Compression of arbitrary messages into fixed length digest, Easy to compute, Pre-image resistance, Second pre-image resistance, Collision resistance, Message Digest (MD),Secure Hash Algorithms (SHAs), Merkle trees, Patricia trees, Distributed hash tables (DHTs), Digital signatures, Elliptic Curve Digital signature algorithm (ECDSA).

Chapter 2, Chapter 3: pg:56-105

Module-3

	Bitcoin, Bitcoin definition, Transactions, The transaction life cycle, The transaction structure, Types of transaction, The structure of a block , The structure of a block header, The genesis block, The bitcoin network, Wallets, Smart Contracts-History, Definition, Ricardian contracts, Smart contract templates, Oracles, Smart Oracles, Deploying smart contracts on a blockchain, The DAO. **Chapter 4:pg:111-148, Chapter 6**
	Module-4
	Ethereum 101, Introduction, Ethereum clients and releases, The Ethereum stack, Ethereum blockchain, Currency (ETH and ETC), Forks, Gas, The consensus mechanism, The world state, Transactions, Contract creation transaction, Message call transaction, Elements of the Ethereum blockchain , Ethereum virtual machine (EVM), Accounts, Block, Ether, Messages, Mining, The Ethereum network. Hands-on: Clients and wallets –Geth. **Chapter 7: pg: 210-227, 235-269**
	Module-5
	Hyperledger, Hyperledger as a protocol, Fabric, Hyperledger Fabric, Sawtooth lake, Corda. **Chapter 9**

Course outcomes (Course Skill Set)

At the end of the course, the student will be able to :

1. Explain the Blockchain terminologies with its applications. design
2. Illustrate the working principles of Blockchain and the Smart Contract Lifecycle
3. Demonstrate the principles and methodologies used in Bitcoin
4. Develop Ethereum Network, Wallets, Nodes, Smart contract and DApps.
5. Make use of Hyperledger in Blockchain Based Application Architecture.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Books

1. Imran Bashir. "Mastring BlockChain", Third Edition, Packt – 2020.

Reference Book

1. Andreas M. , Mastering Bitcoin: Programming the Open Blockchain – O'rielly – 2017.

Web links and Video Lectures (e-Resources):

- https://nptel.ac.in/courses/106104220
- https://www.geeksforgeeks.org/blockchain/
- https://www.tutorialspoint.com/blockchain/index.htm

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Course Project: Covers the implementation of the major concepts outlined in the syllabus– 25 Marks

	Cloud Computing & Security		Semester	VI
	Course Code	**BIS613D**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	3
	Examination type (SEE)	Theory		

Course objectives:

- Introduce the rationale behind the cloud computing revolution and the business drivers
- Understand various models, types and challenges of cloud computing
- Understand the design of cloud native applications, the necessary tools and the design tradeoffs.
- Realize the importance of Cloud Virtualization, Abstraction`s, Enabling Technologies and cloud security

Teaching-Learning Process (General Instructions)

These are sample Strategies; which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.
2. Use of Video/Animation to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
5. Discuss how every concept can be applied to the real world - and when that's possible, it
   helps improve the students' understanding.
6. Use any of these methods: Chalk and board, Active Learning, Case Studies.

Module-1

Distributed System Models and Enabling Technologies: Scalable Computing Over the Internet, Technologies for Network Based Systems, System Models for Distributed and Cloud Computing, Software Environments for Distributed Systems and Clouds, Performance, Security and Energy Efficiency.

Textbook 1: Chapter 1: 1.1 to 1.5

Module-2

Virtual Machines and Virtualization of Clusters and Data Centers: Implementation Levels of Virtualization, Virtualization Structure/Tools and Mechanisms, Virtualization of CPU/Memory and I/O devices, Virtual Clusters and Resource Management, Virtualization for Data Center Automation.

Textbook 1: Chapter 3: 3.1 to 3.5

Module-3

Cloud Platform Architecture over Virtualized Datacenters: Cloud Computing and Service Models, Data Center Design and Interconnection Networks, Architectural Design of

	Compute and Storage Clouds, Public Cloud Platforms: GAE, AWS and Azure, Inter-Cloud Resource Management. **Textbook 1: Chapter 4: 4.1 to 4.5**
	Module-4
	Cloud Security: Top concern for cloud users, Risks, Privacy Impact Assessment, Cloud Data Encryption, Security of Database Services, OS security, VM Security, Security Risks Posed by Shared Images and Management OS, XOAR, A Trusted Hypervisor, Mobile Devices and Cloud Security. **Cloud Security and Trust Management:** Cloud Security Defense Strategies, Distributed Intrusion/Anomaly Detection, Data and Software Protection Techniques, Reputation-Guided Protection of Data Centers. **Textbook 2: Chapter 11: 11.1 to 11.3, 11.5 to 11.8, 11.10 to 11.14** **Textbook 1: Chapter 4: 4.6**
	Module-5
	Cloud Programming and Software Environments: Features of Cloud and Grid Platforms, Parallel and Distributed Computing Paradigms, Programming Support for Google App Engine, Programming on Amazon AWS and Microsoft, Emerging Cloud Software Environments. **Textbook 1: Chapter 6: 6.1 to 6.5**

Course outcome (Course Skill Set)

At the end of the course, the student will be able to:

1. Describe various cloud computing platforms and service providers.
2. Illustrate the significance of various types of virtualization.
3. Identify the architecture, delivery models and industrial platforms for cloud computing based applications.
4. Analyze the role of security aspects in cloud computing.
5. Demonstrate cloud applications in various fields using suitable cloud platforms.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Text Books:

1. Kai Hwang, Geoffrey C Fox, and Jack J Dongarra, Distributed and Cloud Computing, Morgan Kaufmann, Elsevier 2012
2. Dan C. Marinescu, Cloud Computing Theory and Practice, Morgan Kaufmann, 2nd Edition, Elsevier 2018

Reference Books:

1. Rajkumar Buyya, Christian Vecchiola, and Thamrai Selvi, Mastering Cloud Computing McGrawHill Education, 1st Edition, 2017
2. Toby Velte, Anthony Velte, Cloud Computing: A Practical Approach, McGraw-Hill Education, 2017.
3. George Reese, Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, O'Reilly Publication, 1st Edition, 2009
4. John Rhoton, Cloud Computing Explained: Implementation Handbook for Enterprises, Recursive Press, 2nd Edition, 2009.

Web links and Video Lectures (e-Resources):

- https://freevideolectures.com/course/4639/nptel-cloud-computing/1.
- https://www.youtube.com/playlist?list=PLShJJCRzJWxhz7SfG4hpaBD5bKOloWx9J
- https://www.youtube.com/watch?v=EN4fEbcFZ_E
- https://www.youtube.com/watch?v=RWgW-CgdIk0
- https://www.geeksforgeeks.org/virtualization-cloud-computing-types/
- https://www.javatpoint.com/cloud-service-provider-companies

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Installation of virtualization software (Virtual box, Xen etc..) and run applications with different OS. - 10 Marks
- Implement cloud applications using GAE, AWS, Azure/simulate cloud applications using Cloudsim/ Greencloud/ Cloud Analyst etc… - 15 Marks

	FOG AND EDGE COMPUTING		Semester	6
	Course Code	**BCO613D**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	3
	Examination type (SEE)	**Theory**		

Course objectives:

- To understand the students about edge computing, an important branch of distributed computing and IoT with significant applications in Data Science.
- To implement the concepts of fog and cloud computing and exposes students to modern tools and API to deploy relevant infrastructures.

Teaching-Learning Process (General Instructions)

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) needs not to be only a traditional lecture method, but alternative effective teaching methods could be adopted to attain the outcomes.
2. Use of Video/Animation to explain functioning of various concepts.
3. Encourage collaborative (Group Learning) Learning in the class.
4. Ask at least three HOT (Higher order Thinking) questions in the class, which promotes critical thinking.
5. Adopt Problem Based Learning (PBL), which fosters students' Analytical skills, develop design thinking skills such as the ability to design, evaluate, generalize, and analyze information rather than simply recall it.
6. Use animations/videos to help the students to understand the concepts.

Module-1

Fog computing requirements when applied to IoT: Scalability, Interoperability, Fog- IoT architectural model, Challenges on IoT Stack Model via TCP/IP Architecture, Data Management, filtering, Event Management, Device Management, cloudification, virtualization, security and privacy issues. Integrating IoT, Fog, Cloud Infrastructures: Methodology, Integrated C2F2T Literature by Modelling Technique by Use-Case Scenarios, Integrated C2F2T Literature by Metrics.

Textbook 1: Ch: 3, 3.3, 3.4, 3.5

Module-2

Exploiting Fog Computing in Health Monitoring: An Architecture of a Health Monitoring IoT- Based System with Fog Computing, Fog Computing Services in Smart E-Health Gateways, Discussion of Connected Components.

Fog Computing Model for Evolving Smart Transportation Applications: Introduction, Data-Driven Intelligent Transportation Systems, Fog Computing for Smart Transportation Applications Case Study: Intelligent Traffic Lights Management (ITLM) System.

Textbook 1: Ch: 12, 12.2, 12.3, 14.2, 14.5, 14.6

Module-3

Software Defined Networking and application in Fog Computing: Open Flow Protocol, Open Flow Switch, SDN in Fog Computing, Home Network using SDN. Security and Privacy issues: Trust and privacy issues in IoT Network, web Semantics and trust Management for Fog Computing, Machine Learning based security in Fog Computing, Cyber- Physical Energy Systems over Fog Computing.

Textbook2: Ch: 5.6, 16.2, 16.2.1, 16.4, 16.6.4

	Module-4
	Introduction to Edge Computing Scenarios and Use cases - Edge computing purpose and definition, Edge computing use cases, Edge computing hardware architectures, Edge platforms, Edge vs Fog Computing, Communication Models - Edge, Fog, and M2M. **Textbook 3: Ch:8**
	Module-5
	IoT Architecture and Core IoT Modules-A connected ecosystem, IoT versus machine-to-machine versus, SCADA, The value of a network and Metcalfe's and Beckstrom's laws, IoT and edge architecture, Role of an architect, Understanding Implementations with the examples- Edge computing with RaspberryPi, Industrial, and Commercial IoT and Edge, and Edge computing and solutions. **Textbook 3: Ch:2**

Course outcome (Course Skill Set)

At the end of the course, the student will be able to :

1. Explore the need for new computing paradigms.
2. Explain the major components of fog and edge computing architectures.
3. Identify potential technical challenges of the transition process and suggest solutions.
4. Analyze data and application requirements and pertaining issues.
5. Compare design and model infrastructures.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assessment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned. Implementation of Image processing and video processing techniques in Java/Python/Matlab is recommended.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.

3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Textbooks

1. Satish Narayana Srirama and Rajkumar Buyya, Fog and Edge Computing: Principles and Paradigms, (Wiley Series on Parallel and Distributed Computing), 2019.
2. Assad Abbas, Samee U. Khan, Albert Y. Zomaya. Fog Computing: Theory and Practice, Wiley 2020.
3. Perry Lea, IoT and Edge Computing for Architects - Second Edition, Publisher: Packt Publishing, 2020, ISBN: 9781839214806.

Reference books

1. Shanhe Yi, Cheng Li, Qun Li, ―A Survey of Fog Computing: Concepts, Applications and Issues‖, Mobidata'15, ACM 978-1-4503-3524-9/15/06, DOI: 10.1145/2757384.2757397, June 21, 2015, Hangzhou, China.

2. Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli, ―Fog Computing and Its Role in the Internet of Things‖, MCC'12, August 17, 2012, Helsinki, Finland, ACM, 2012.

3. Raspberry Pi Cookbook, 3rd Edition, by Simon Monk, Publisher: O'Reilly Media, Inc., 2019, ISBN: 978149204322.

4. David Jensen, "Beginning Azure IoT Edge Computing: Extending the Cloud to the Intelligent Edge, MICROSOFT AZURE.

Web links and Video Lectures (e-Resources):

- https://archive.nptel.ac.in/courses/106/104/106104242/
- https://onlinecourses.nptel.ac.in/noc24_cs66/preview

Activity Based Learning (Suggested Activities in Class)/Practical-Based Learning

- Assignment-1 (group of 4): A literature survey report and review map (refer to recent min. 10 indexed journal papers) on fog computing techniques. 15 Marks
- Assignment-2 (group of 4): A literature survey report and review map (refer to recent min. 10 indexed journal papers) on edge computing techniques. 15 Marks

	Wireless and Mobile Device Security		Semester	VI
	Course Code	**BCY613D**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03
	Examination type (SEE)	Theory		

Course objectives:

- Understand the evolution of wired and wireless networks and their societal and economic impacts.
- Learn about mobile communication technologies and associated security challenges.
- Analyse WLAN fundamentals, vulnerabilities, and threat scenarios.
- Explore security measures for WLANs and mobile devices.
- Gain proficiency in risk assessment and security tools for wireless networks.

Teaching-Learning Process (General Instructions)

These are sample strategies; which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.
2. Utilize video/animation films to illustrate the functioning of various concepts.
3. Promote collaborative learning (Group Learning) in the class.
4. Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.
5. Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.
6. Introduce topics through multiple representations.
7. Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.
8. Discuss the real-world applications of every concept to enhance students' comprehension.
9. Use any of these methods: Chalk and board, Active Learning, Case Studies.

Module-1 8 Hours

Evolution of Data and Wired Networking

The Evolution of Data Networks: The Dawn of Data Communication; Early Data Networks; The Internet Revolution; Advances in Personal Computers and Mobile Phones; Computers Go Mobile; Convergence of Mobile and Data Networks; Business Challenges Addressed by Wireless Networking; IP Mobility and BYOD Impact; Security Considerations and Cybercrime Evolution;

The Evolution of Wired Networking to Wireless Networking: Networking and OSI Reference Model; Layers of the OSI Model; Transition from Wired to Wireless Networking; Economic Impact of Wireless Networking; Applications in Health Care, Warehousing, Retail, and Knowledge Work; WiFi Impact on Developing Nations and IoT Introduction

Module-2 8 Hours

	The Mobile Revolution and Security Threats **The Mobile Revolution:** Cellular Communication and Coverage; Frequency Sharing and Handoff; Evolution of Mobile Networks (1G to 4G/LTE); BYOD and Economic Impact of Mobility; Business Use Cases for Mobile Networking; **Security Threats Overview:** Threat Categories: Confidentiality, Integrity, Availability; Wireless and Mobile Device Threats: Data Theft, System Access; Risk Mitigation and BYOD for SMBs; Security Standards and Regulatory Compliance (ISO, NIST, PCI DSS);
	Module-3 8 Hours
	WLAN Fundamentals and Threat Analysis: **How Do WLANs Work?** WLAN Topologies, Service Sets, and Standards; Wireless Access Points (WAPs) and Antennas; Coverage Area Determination and Site Surveys; Spectrum and Protocol Analysis; **WLAN and IP Networking Threat and Vulnerability Analysis:** Types of Attackers: Insiders vs. Outsiders; Physical Security, Social Engineering, and Wardriving; Rogue Access Points and Bluetooth Vulnerabilities; Malicious Data Insertion, Denial of Service, and Peer to Peer Hacking;
	Module-4 Hours
	WLAN Security Measures **Basic WLAN Security Measures:** Design and Implementation for Security; Authentication, MAC Filters, VPN, and VLANs; Wired Equivalent Privacy, WPA, WPA2; Ongoing Management Considerations (Firmware, Physical Security); **Advanced WLAN Security Measures:** Comprehensive Security Policies; Authentication and Access Control (EAP, RADIUS); Intrusion Detection/Prevention Systems and Protocol Filtering; Advanced Data Protection: WPA2 Modes, VPN, IPsec; User Segmentation, VLANs, DMZ Segmentation; Device and Network Management;
	Module-5 8 Hours
	Advanced Mobile Security and Risk Management **WLAN Auditing Tools:** Discovery Tools (NetStumbler, Kismet); Penetration Testing Tools (Metasploit, Aircrackng); Network Enumerators, Protocol Analyzers, and Attack Tools; **WLAN and IP Network Risk Assessment:** Risk Assessment Methodologies and Stages; Security Risk Analysis and Audits; Legal Requirements and IT Security Management; **Mobile Communication Security Challenges:** Mobile Phone Threats: Exploits, Tools, and Techniques; Security Architectures: Android, iOS, Windows Phone; BYOD and Enterprise Mobility Management; **Mobile Device Security Models:** Security Models: Android, iOS, Windows Phone; Device Management, Encryption, and Handoff Challenges;

Course outcome (Course Skill Set)

At the end of the course, the student will be able to:

1. Explain the evolution and impact of wired and wireless networks.

2. Identify and categorize security threats to wireless and mobile networks.
3. Design and implement security measures for WLANs and mobile devices.
4. Utilize security tools for auditing and penetration testing.
5. Develop strategies to manage risks in mobile and wireless communication systems.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Text book

1. J. Doherty, Wireless and Mobile Device Security. Jones & Bartlett Learning, 2nd edition Dec. 2021.

Reference Books:

Reference book

1. M. S. Obaidat, A. Anpalagan, I. Woungang, and S. Misra, *Security and Privacy in Wireless and Mobile Networks*. MDPI, 2021.
2. M. Zinkus, T. M. Jois, and M. Green, "Data Security on Mobile Devices: Current State of the Art, Open Problems, and Proposed Solutions," *arXiv*, 2021. [Online]. Available: https://arxiv.org/abs/2105.12613
3. J. Stevenson, Mobile Offensive Security Pocket Guide: A Quick Reference Guide for Android and iOS. Independently Published, 2022.

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

1. Use any WLAN simulator tools to demonstrate the working of RADIUS protocol (10 marks)
2. Students in a group of TWO or THREE are expected to prepare report on different Intrusion Detection and Prevention techniques. (15)

	INTRODUCTION TO DATA STRUCTURES		Semester	6
	Course Code	**BCS654A**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03
	Examination type (SEE)	Theory		

Course Objectives:

- Introduce primitive and non-primitive data structures
- Understand the various types of data structure along their operations
- Study various searching and sorting algorithms
- Assess appropriate data structures during program development / problem solving

Teaching-Learning Process (General Instructions)

These are sample strategies; which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.
2. Utilize video/animation films to illustrate the functioning of various concepts.
3. Promote collaborative learning (Group Learning) in the class.
4. Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.
5. Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.
6. Introduce topics through multiple representations.
7. Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.
8. Discuss the real-world applications of every concept to enhance students' comprehension.
9. Use any of these methods: Chalk and board, Active Learning, Case Studies.

Module-1

Arrays: Introduction, One-Dimensional Arrays, Two-Dimensional Arrays, Initializing Two-Dimensional Arrays, Multidimensional arrays.

Pointers: Introduction, Pointer Concepts, Accessing Variables through Pointers, Pointer Applications, Dynamic Memory Allocation Functions.

Structures and Unions: Introduction, Declaring Structures, Giving Values to Members, Structure Initialization, Comparison of Structure Variables, Arrays of Structures, Arrays within Structures, Nested Structures, Unions, Size of Structures.

Textbook 1: Ch. 8.1 to 8.5, Ch. 12.1 to 12.8, 12.10, 12.11.
Textbook 2: Ch. 2.1 to 2.3, 2.5, 2.9.

Module-2

	Stacks: Introduction, Stack Operations, Stack Implementation using Arrays, Applications of Stacks. **Queues:** Introduction, Queue Operations, Queue Implementation using Arrays, Different Types of Queues: Circular Queues, Double-Ended Queues, Priority Queues, Applications of Queues. **Textbook 2:** Ch. 6.1 to 6.3, Ch. 8.1 to 8.2.
	Module-3
	Linked Lists: Introduction, Singly Linked List, Self-Referential Structures, Operations on Singly Linked Lists: Insert-Delete-Display, Implementation of Stacks and Queues using Linked List, Concatenate two Lists, Reverse a List without Creating a New Node, Static Allocation Vs Linked Allocation. **Circular Singly Linked List:** Introduction, Operations: Insert-Delete-Display. **Textbook 2:** Ch. 9.1 to 9.2, 9.3 (Only 9.3.1 to 9.3.5, 9.3.11 to 9.3.12), 9.4 to 9.5.
	Module-4
	Trees: Introduction, Basic Concepts, Representation of Binary Trees, Operations on Binary Trees: Insertion-Traversals-Searching-Copying a Tree, Binary Search Trees, Operations on Binary Search Trees: Insertion-Searching-Find Maximum and Minimum Value-Count Nodes, Expression Trees. **Textbook 2:** Ch. 10.1 to 10.4, 10.5 (Only 10.5.1, 10.5.2, 10.5.3.1, 10.5.3.2, 10.5.3.4), 10.6.3.
	Module-5
	Sorting: Introduction, Bubble Sort, Selection Sort, Insertion Sort. **Searching:** Introduction, Linear Search, Binary Search. **Textbook 1:** Ch. 17.1, 17.2.6, 17.3.2. **Textbook 2:** Ch. 11.1 to 11.3, 11.10.1.

Course outcome (Course Skill Set)

At the end of the course, the student will be able to:

1. Develop C programs utilizing fundamental concepts such as arrays, pointers and structures.
2. Apply data structures like stacks and queues to solve problems.
3. Develop C programs using linked lists and their various types.
4. Explain the fundamental concepts of trees and their practical applications.
5. Demonstrate different sorting and searching algorithms and determine their algorithmic complexities.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Text Books:

1. E Balagurusamy, "C Programming and Data Structures", 4th Edition, McGraw-Hill, 2007.
2. A M Padma Reddy, "Systematic Approach to Data Structures using C", 9th Revised Edition, Sri Nandi Publications, 2009.

Reference Books:

1. Ellis Horowitz and Sartaj Sahni, "Fundamentals of Data Structures in C", 2nd Edition, Universities Press, 2014.
2. Seymour Lipschutz, "Data Structures Schaum's Outlines", Revised 1st Edition, McGraw-Hill, 2014.

Web links and Video Lectures (e-Resources):

- https://www.youtube.com/watch?v=DFpWCl_49i0
- https://www.youtube.com/watch?v=x7t_-ULoAZM
- https://www.youtube.com/watch?v=I37kGX-nZEI
- https://www.youtube.com/watch?v=XuCbpw6Bj1U
- https://www.youtube.com/watch?v=R9PTBwOzceo

- https://www.youtube.com/watch?v=qH6yxkw0u78
- https://archive.nptel.ac.in/courses/106/105/106105085/
- https://onlinecourses.swayam2.ac.in/cec19_cs04/preview

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

Develop C programs that focus on Data Structure concepts such as arrays, pointers, structures, stacks, queues, linked lists, trees as well as, sorting and searching algorithms (25 Marks).

	FUNDAMENTALS OF OPERATING SYSTEMS		Semester	6
	Course Code	**BCS654B**	CIE Marks	50
	Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	03
	Examination type (SEE)	Theory		

Course objectives:

- To demonstrate the need and different types of OS
- To discuss suitable techniques for management of different resources
- To analyse different memory, storage, and file system management strategies.

Teaching-Learning Process (General Instructions)

These are sample strategies; which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.
2. Utilize video/animation films to illustrate the functioning of various concepts.
3. Promote collaborative learning (Group Learning) in the class.
4. Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.
5. Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.
6. Introduce topics through multiple representations.
7. Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.
8. Discuss the real-world applications of every concept to enhance students' comprehension.
9. Use any of these methods: Chalk and board, Active Learning, Case Studies.

Module-1

Introduction: What operating systems do; Computer System organization; Computer System Organization, Computer System architecture; Operating System operations; Resource Management

Operating System Structures: Operating System Servies, User and Operating System interface; System calls, Application Program Interface, Types of system calls;

Textbook 1: Chapter 1: 1.1, 1.2, 1.3,1.4, 1.5 Chapter 2: 2.1, 2.2 (2.2.1, 2.2.2), 2.3 (2.3.2, 2.3.3)

Module-2

Process Management: Process concept; Process scheduling; Operations on processes; Interprocess Communication

Multi-threaded Programming: Overview; Multithreading models, Thread Libraries

Textbook 1: Chapter 3: 3.1-3.4, Chapter 4: 4.1, 4.3 5, 4.4

Module-3

	CPU Scheduling: Basic Concepts, Scheduling criteria, Scheduling algorithms, Thread Scheduling**,** **Process Synchronization:** Synchronization: The critical section problem; Peterson's solution; Semaphores; Classical problems of synchronization; **Textbook 1: Chapter 5: 5.1, 5.2,5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.4 Chapter 6: 6.1, 6.2.,6.3, 6.6**
	Module-4
	Deadlocks: System model; Deadlock characterization; Methods for handling deadlocks; Deadlock prevention; Deadlock avoidance; Deadlock detection and recovery from deadlock. **Memory Management:** Background; Contiguous memory allocation; Paging; Structure of page table **Textbook 1: Chapter 8: 8.1-8.8 Textbook 1: Chapter 9: 9.1-9.4 (9.4.1, 9.4.2)**
	Module-5
	Virtual Memory Management: Background; Demand paging; Copy-on-write; Page replacement; **File System Interface:** File concept; Access methods; Directory Structure, Protection, File System Implementation: File System Structure, File System Operations, **File System Internals**: File Systems, File System Mounting; Partition and Mounting, File sharing; **Textbook 1: Chapter 10: 10.1-10.3, 10.4 (10.4.1, 10.4.2, 10.4.4.) Chapter 13: 13.1, 13.2, 13.3 (13.3.1, 13.3.2, 13.3.3), 13.4 (13.4.1, 13.4.2) Chapter 15: 15.1-15.4**

Course outcomes (Course Skill Set)

At the end of the course, the student will be able to:

1. Explain the fundamentals of operating systems.
2. Apply appropriate CPU scheduling algorithm for the given scenarios.
3. Analyse the various techniques for process synchronization and deadlock handling.
4. Apply the various techniques for memory management
5. Analyse the importance of File System Mounting and File Sharing

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Text Books:

1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Operating System Principles 10th edition, Wiley-India, 2015

Reference Books

2. Ann McHoes Ida M Fylnn, Understanding Operating System, Cengage Learning, 6th Edition, 2010
3. D.M Dhamdhere, Operating Systems: A Concept Based Approach 3rd Ed, McGraw-Hill, 2013, P.C.P. Bhatt, An Introduction to Operating Systems: Concepts and Practice 4th Edition, PHI(EEE), 2014.
4. William Stallings Operating Systems: Internals and Design Principles, 6th Edition, Pearson, 2008

Reference Books:

1. Akshay Kulkarni, Adarsha Shivananda, "Natural Language Processing Recipes - Unlocking Text Data with Machine Learning and Deep Learning using Python", Apress, 2019.
2. T V Geetha, "Understanding Natural Language Processing – Machine Learning and Deep Learning Perspectives", Pearson, 2024.

3. Gerald J. Kowalski and Mark.T. Maybury, “Information Storage and Retrieval systems”, Kluwer Academic Publishers.

Web links and Video Lectures (e-Resources):

1.https://archive.nptel.ac.in/courses/106/105/106105214/
2.https://archive.nptel.ac.in/courses/106/102/106102132/

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Students are expected to prepare animated PPT to illustrate the different types of Process Scheduling and Paging. **(10 Marks)**
- Students are required to prepare detailed case study report on Deadlocks **OR** Students can illustrate deadlock using any programming language **(15 Marks)**

	MOBILE APPLICATION DEVELOPMENT		Semester	6
	Course Code	BIS654C	CIE Marks	50
	Teaching Hours/Week (L:T:P: S)	3:0:0	SEE Marks	50
	Total Hours of Pedagogy	40	Total Marks	100
	Credits	03	Exam Hours	3
	Examination type (SEE)	Theory		

Course objectives:

Create, test and debug Android application by setting up Android development environment.

Implement adaptive, responsive user interfaces that work across a wide range of devices.

Infer long running tasks and background work in Android applications

Demonstrate methods in storing, sharing and retrieving data in Android applications

Analyze performance of android applications

Describe the steps involved in publishing Android application to share with the world.

Teaching-Learning Process (General Instructions)

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Chalk and board, power point presentations
2. Online material (Tutorials) and video lectures.
3. Demonstration of setup Android application development environment & programing examples.
4. Illustrate user interfaces for interacting with apps and triggering actions

Module-1

Introduction to Android OS: Android Description – Open Handset Alliance – Android. Ecosystem – Android versions – Android Activity – Features of Android – Android Architecture Stack Linux Kernel. Configuration of Android Environment: Operating System – Java JDK Android SDK – Android Development Tools (ADT) – Android Virtual Devices (AVDs) – Emulators Dalvik Virtual Machine – Differences between JVM and DVM – Steps to Install and Configure Eclipse and SDK.

(Chapters 1 & 2)

Module-2

Create the first android application: Directory Structure. Android User Interface: Understanding the Components of a screen– Linear Layout – Absolute Layout – Frame. Layout Relative Layout – Table Layout.

(Chapters 3 & 4)

Module-3

Designing User Interface with View – Text View – Button – Image Button – Edit Text Check Box – Toggle Button – Radio Button and Radio Group – Progress Bar – Auto complete Text View – Spinner – List View – Grid View – Image View - Scroll View – Custom Toast – Alert – Time and Date Picker. (Chapter 5)
Module-4
Activity: Introduction – Intent – Intent filter – Activity life cycle – Broadcast life cycle Service. Multimedia: Android System Architecture – Play Audio and Video – Text to Speech. (Chapters 6 & 7)
Module-5
SQLite Database in Android: SQLite Database – Creation and Connection of the database – Transactions. Case Study: SMS Telephony and Location Based Services. (Chapters 8, 9, & 10)
Course outcome (Course Skill Set) At the end of the course the student will be able to: 1. Explain Mobile Application Ecosystem like concepts, architecture, and lifecycle of mobile applications on Android 2. Identify the key components of mobile application frameworks and development tools. 3. Apply design principles to create intuitive and responsive user interfaces using appropriate UI/UX tools. 4. Develop Functional Mobile Applications -Integrate core functionalities such as layouts, event handling, navigation, and multimedia support into applications. 5. Implement local data storage mechanisms (SQLite, Shared Preferences) and external databases (Firebase, APIs) for mobile applications.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous internal Examination (CIE)

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examinations (SEE)

SEE paper shall be set for 50 questions, each of the 01 marks. The pattern of the question paper is MCQ (multiple choice questions). The time allotted for SEE is **01 hour.** The student has to secure a minimum of 35% of the maximum marks meant for SEE.

OR

MCQ (Multiple Choice Questions) are preferred for 01 credit courses, however, if course content demands the general question paper pattern that followed for 03 credit course, then

1. The question paper will have ten questions. Each question is set for 10 marks.
2. There will be 2 questions from each module. Each of the two questions under a module may or may not have the sub-questions (with maximum sub-questions of 02, with marks distributions 5+5, 4+6, 3+7).
3. The students have to answer 5 full questions, selecting one full question from each module.

Suggested Learning Resources:

Books

1. TEXT BOOK 1. Prasanna Kumar Dixit, "Android", Vikas Publishing House Private Ltd., Noida, 2014.
2. REFERENCE BOOKS
   1. Reto Meier and Wrox Wiley, "Professional Android 4 Application Development", 2012.
   2. ZiguradMednieks, LaridDornin, G.BlakeMeike, Masumi Nakamura, "Programming Andriod", O'Reilly,2013.
   3. Robert Green, Mario Zechner, "Beginning Android 4 Games Development", Apress Media LLC, New York, 2011

Web links and Video Lectures (e-Resources):

	• .https://www.geeksforgeeks.org/android-tutorial/ • https://developer.android.com/ • https://www.tutorialspoint.com/android • https://www.w3schools.blog/android-tutorial
	Activity Based Learning (Suggested Activities in Class)/Practical-Based Learning: 1. Programming exercises, fostering the practical application of theoretical concepts. [25 marks]

INTRODUCTION TO ARTIFICIAL INTELLIGENCE		Semester	6
Course Code	**BAI654D**	CIE Marks	50
Teaching Hours/Week (L: T:P: S)	3:0:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03
Examination type (SEE)	Theory		

Course objectives:

- To understand the primitives of AI
- To familiarize Knowledge Representation Issues
- To understand fundamentals of Statistical Reasoning, Natural Language Processing.

Teaching-Learning Process (General Instructions)

These are sample strategies; which teachers can use to accelerate the attainment of the various course outcomes.

1. Lecturer method (L) does not mean only the traditional lecture method, but different types of teaching methods may be adopted to achieve the outcomes.
2. Utilize video/animation films to illustrate the functioning of various concepts.
3. Promote collaborative learning (Group Learning) in the class.
4. Pose at least three HOT (Higher Order Thinking) questions in the class to stimulate critical thinking.
5. Incorporate Problem-Based Learning (PBL) to foster students' analytical skills and develop their ability to evaluate, generalize, and analyze information rather than merely recalling it.
6. Introduce topics through multiple representations.
7. Demonstrate various ways to solve the same problem and encourage students to devise their own creative solutions.
8. Discuss the real-world applications of every concept to enhance students' comprehension.
9. Use any of these methods: Chalk and board, Active Learning, Case Studies

Module-1

What **is** artificial intelligence? Problems, Problem Spaces, and search

Text Book 1: Ch 1, 2

Module-2

Knowledge Representation Issues, Using Predicate Logic, representing knowledge using Rules.

Text Book 1: Ch 4, 5 and 6.

Module-3

Symbolic Reasoning under Uncertainty, Statistical reasoning

Text Book 1: Ch 7, 8

Module-4

Game Playing, Natural Language Processing

Text Book 1: Ch 12 and 15

Module-5

Learning, Expert Systems.

Text Book 1: Ch 17 and 20

Course outcomes (Course Skill Set)

At the end of the course, the student will be able to:

1. Identify the problems where the adaptation of AI has significant impact.
2. Analyse the different approaches of Knowledge Representation.
3. Explain Symbolic Reasoning under Uncertainty and Statistical reasoning.
4. Derive the importance of different types of Learning Techniques.
5. Explain Natural Language Processing and Expert System.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

- For the Assignment component of the CIE, there are 25 marks and for the Internal Assessment Test component, there are 25 marks.
- The first test will be administered after 40-50% of the syllabus has been covered, and the second test will be administered after 85-90% of the syllabus has been covered
- Any two assignment methods mentioned in the 22OB2.4, if an assignment is project-based then only one assignment for the course shall be planned. The teacher should not conduct two assignments at the end of the semester if two assignments are planned.
- For the course, CIE marks will be based on a scaled-down sum of two tests and other methods of assessment.

Internal Assessment Test question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester-End Examination:

Theory SEE will be conducted by University as per the scheduled timetable, with common question papers for the course (**duration 03 hours).**

1. The question paper will have ten questions. Each question is set for 20 marks.
2. There will be 2 questions from each module. Each of the two questions under a module (with a maximum of 3 sub-questions), **should have a mix of topics** under that module.
3. The students have to answer 5 full questions, selecting one full question from each module.
4. Marks scored shall be proportionally reduced to 50 marks

Suggested Learning Resources:

Text Books:

1. E. Rich, K. Knight & S. B. Nair, Artificial Intelligence, 3rd Edition, McGraw Hill.,2009

Reference Books

2. Stuart Rusell, Peter Norving, Artificial Intelligence: A Modern Approach, 2nd Edition, Pearson Education

3. Dan W. Patterson, Introduction to Artificial Intelligence and Expert Systems, 1st Edition,Prentice Hal of India, 2015
4. G. Luger, Artificial Intelligence: Structures and Strategies for complex problem Solving, 4th Edition, Pearson Education, 2002.
5. N.P. Padhy "Artificial Intelligence and Intelligent Systems", Oxford University Press, 2015

Web links and Video Lectures (e-Resources):

1. https://nptel.ac.in/courses/106102220
2. https://nptel.ac.in/courses/106105077
3. https://archive.nptel.ac.in/courses/106/105/106105158/
4. https://archive.nptel.ac.in/courses/106/106/106106140/

Activity Based Learning (Suggested Activities in Class)/ Practical Based learning

- Apply NLP steps for any given real time scenario. Students are expected to document different NLP steps and their output for the given scenario. Students can use python or any programming language of their choice. **(10 Marks)**
- Students are expected to identify different case studies/scenarios where expert systems can be adopted. Students need to prepare a report on any one case study. **(15 marks)**

Vulnerability Assessment Penetration Testing Laboratory		Semester	VI
Course Code	**BICL606**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	0:0:2:0	SEE Marks	50
Credits	01	Exam Hours	100
Examination type (SEE)	Practical		

Course objectives:

- To get Practical exposure of Network Reconnaissance and Vulnerability Scanning
- Exploiting a Known Vulnerability
- To get Practical exposure on SQL Injection attacks and Cross site Scripting Attacks
- To get Practical exposure on Password Cracking and Penetration Testing

Sl.NO	Experiments
1	**Experiment 1: Network Reconnaissance & Footprinting** Scenario: An organization, "TechSecure Corp," suspects that its internal LAN might contain devices with unpatched services. As an external consultant with limited initial knowledge, your first step is to gain intelligence about the network. You have been given a subnet range and must map out devices and open ports. Tasks: - Use Nmap for host discovery, port scanning, and service enumeration. - Employ Recon-ng or Amass for passive reconnaissance to discover hostnames, subdomains, or metadata. - Document identified hosts, operating systems, and running services. Deliverable: A network inventory report listing IP addresses, OS guesses, and active services.
2	**Experiment 2: Vulnerability Scanning & Assessment** Scenario: After mapping the network, you've discovered a web server and a file-sharing server. Management wants a vulnerability assessment of these targets to identify known weaknesses before attackers can exploit them. Tasks: - Use OpenVAS to perform a comprehensive vulnerability scan on a Linux-based server (Metasploitable 2). - Run Nikto against the web application (e.g., DVWA) to find outdated server software, dangerous file uploads, or default credentials. - Assess the severity and relevance of each discovered vulnerability. Deliverable: A vulnerability assessment report with CVE references and risk ratings.

3	**Experiment 3: Exploiting a Known Vulnerability** Scenario: Your scan found a critical vulnerability on a target server (e.g., Metasploitable 2's vsftpd backdoor). The organization wants proof-of-concept exploitation to understand the potential damage if a malicious actor leverages this flaw. Tasks: - Use the Metasploit Framework to exploit the known vulnerability and obtain a shell. - Verify the level of access gained and the data potentially exposed. Deliverable: A screenshot and log of a successful exploit session, and notes on potential impact. Deliverable: A screenshot and log of a successful exploit session, and notes on potential impact.
4	**Experiment 4: SQL Injection Attacks on Web Applications** Scenario: The DVWA application's login and search functionalities are suspected to lack proper input validation. The company needs confirmation that attackers can extract sensitive data using SQL injection. Tasks: - Use SQLMap against DVWA's vulnerable pages to enumerate databases, tables, and potentially user credentials. - Confirm that an attacker could retrieve confidential information from the backend database. Deliverable: Proof (screenshots/logs) of extracted database entries and a brief report on the risk to the organization.
5	**Experiment 5: Cross-Site Scripting (XSS) Attacks** Scenario: The OWASP Juice Shop allows user-generated content. The security team suspects there is an XSS flaw that could lead to user session hijacking or credential theft. Tasks: - Inject a malicious JavaScript payload via a form or comment section using Burp Suite Community Edition or OWASP ZAP to intercept and modify requests. - Demonstrate that the payload executes in a victim's browser (e.g., by producing an alert or stealing cookies). Deliverable: A screenshot of the XSS payload executing and a short explanation of the potential consequences.

6	**Experiment 6: Password Cracking & Credential Harvesting** Scenario: From a previous SQL injection attack, you have obtained a list of hashed passwords. The concern is that weak passwords allow attackers to pivot within the network. Tasks: - Use John the Ripper or Hashcat to crack the obtained hashes. - Alternatively, if allowed, use Hydra to brute-force SSH or FTP logins on Metasploitable 2. - Evaluate how easily an attacker could escalate their access. Deliverable: A list of cracked passwords or confirmed account access, along with complexity recommendations.
7	**Experiment 7: Wireless Network Security Assessment (Optional)** Scenario: TechSecure Corp provides a guest Wi-Fi network secured with WPA2. They want to ensure their wireless environment cannot be easily compromised by a nearby attacker. Tasks: - Use Aircrack-ng to capture the WPA2 handshake. - Attempt to crack the passphrase with a dictionary-based attack to assess wireless password strength. Deliverable: A report detailing if the WPA2 passphrase was recovered and suggestions for stronger wireless security.
8	**Experiment 8: Privilege Escalation on a Compromised Host** Scenario: You have a non-privileged shell on a compromised Linux server. The security team wants to know if gaining full root access is feasible, helping them understand post-exploitation risks. Tasks: - Use LinPEAS or Linux Exploit Suggester to find local privilege escalation opportunities. - Exploit a vulnerable kernel or misconfigured SUID binary to become root. Deliverable: Evidence (screenshot of id command) that you obtained root privileges, and a short write-up of the exploited issue.
9	**Experiment 9: Full Web Application Penetration Test** Scenario: You must perform a comprehensive test against the OWASP Juice Shop. The organization wants a detailed understanding of all web vulnerabilities before deployment. Tasks: - Use OWASP ZAP to spider and scan the application. - Identify various vulnerabilities (XSS, SQLi, broken authentication, insecure direct object

	references) and exploit them. - Summarize the findings and recommend remediations. Deliverable: A full web application penetration test report, including identified vulnerabilities, exploitation proofs, and remediation steps.
10	**Experiment 10: Reporting & Remediation Strategy** Scenario: After completing all tests, you must present your findings to the executive board and the technical team. The final deliverable should translate technical details into actionable insights. Tasks: - Consolidate all findings from previous experiments into a structured, professional VAPT report. - Include vulnerability descriptions, risk ratings, proofs of concept, and recommended mitigations. - Provide a roadmap for future hardening and security improvements Deliverable: A polished final report (PDF or Markdown) that can be understood by both management and IT staff, outlining the security posture, identified weaknesses, and steps for remediation.

Course outcomes:

At the end of the course the student will be able to:

- Implement Network Reconnaissance , Vulnerability Scanning and assessment.
- Demonstrate the working of Password Cracking, Reporting and Remediation strateg.
- Implement Full web applications penetration Testing .
- Experiment with Cross Site Scripting Attacks and SQL Injection attacks.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together

Continuous Internal Evaluation (CIE):

CIE marks for the practical course are **50 Marks**.

The split-up of CIE marks for record/ journal and test are in the ratio **60:40**.

- Each experiment is to be evaluated for conduction with an observation sheet and record write-up. Rubrics for the evaluation of the journal/write-up for hardware/software experiments are designed by the faculty who is handling the laboratory session and are made known to students at the beginning of the practical session.
- Record should contain all the specified experiments in the syllabus and each experiment write-up will be evaluated for 10 marks.
- Total marks scored by the students are scaled down to **30 marks** (60% of maximum marks).
- Weightage to be given for neatness and submission of record/write-up on time.
- Department shall conduct a test of 100 marks after the completion of all the experiments listed in the syllabus.
- In a test, test write-up, conduction of experiment, acceptable result, and procedural knowledge will carry a weightage of 60% and the rest 40% for viva-voce.
- The suitable rubrics can be designed to evaluate each student's performance and learning ability.
- The marks scored shall be scaled down to **20 marks** (40% of the maximum marks).

The Sum of scaled-down marks scored in the report write-up/journal and marks of a test is the total CIE marks scored by the student.

Semester End Evaluation (SEE):

- SEE marks for the practical course are 50 Marks.
- The examination schedule and names of examiners are informed to the university before the conduction of the examination. These practical examinations are to be conducted between the schedule mentioned in the academic calendar of the University.
- All laboratory experiments are to be included for practical examination.
- (Rubrics) Breakup of marks and the instructions printed on the cover page of the answer script to be strictly adhered to by the examiners. **OR** based on the course requirement evaluation rubrics shall be decided jointly by examiners.
- Students can pick one question (experiment) from the questions lot prepared by the examiners jointly.

- Evaluation of test write-up/ conduction procedure and result/viva will be conducted jointly by examiners.

General rubrics suggested for SEE are mentioned here, writeup-20%, Conduction procedure and result in -60%, Viva-voce 20% of maximum marks. SEE for practical shall be evaluated for 100 marks and scored marks shall be scaled down to 50 marks (however, based on course type, rubrics shall be decided by the examiners)

Change of experiment is allowed only once and 15% of Marks allotted to the procedure part are to be made zero.

The minimum duration of SEE is 02 hours

Suggested Learning Resources:

Textbooks

1. M. Scheffler, Hacking and Security: The Comprehensive Guide to Penetration Testing and Cybersecurity. Addison-Wesley, 2022.
2. M. Chapple and D. Seidl, CompTIA PenTest+ Study Guide: Exam PT0-002. Wiley, 2021.

Reference books

S. Rahalkar, *Metasploit 5.0 for Beginners: Perform Penetration Testing to Secure Your IT Environment Against Threats and Vulnerabilities*. Packt Publishing, 2020.

Websites:

1. TryHackMe, "Cybersecurity Training Platform," [Online]. Available: https://tryhackme.com/.
2. Hack The Box, "Online Penetration Testing Lab," [Online]. Available: https://www.hackthebox.com/.

Infrastructure Requirements:

A hypervisor (e.g., VirtualBox or VMware) installed on a host machine with at least 8 GB RAM, 250 GB of disk space, and internet connectivity for initial setup.
- A virtual network isolated from the host's primary LAN to prevent unintended impact.
- Attacker VM: Kali Linux (latest version), pre-installed with common pentest tools.
- Target VMs

1. Metasploitable 2: An intentionally vulnerable Linux server.
3. Damn Vulnerable Web Application (DVWA): A purposefully flawed web app for testing web vulnerabilities.
4. OWASP Juice Shop: An intentionally insecure modern web application.
5. A custom Linux or Windows VM: For privilege escalation and service misconfiguration scenarios.
6. A simulated WPA2 wireless network (optional, if WLAN testing is feasible within the lab environment).

Open Source Tools:

- Recon and Enumeration: Nmap, Amass, Recon-ng
- Vulnerability Scanning: OpenVAS, Nikto, OWASP ZAP
- Web Exploitation: Burp Suite Community Edition, SQLMap, XSStrike
- Exploitation Framework: Metasploit Framework
- Password Attacks: John the Ripper, Hashcat, Hydra
- Wireless Attacks (If applicable): Aircrack-ng
- Privilege Escalation Enumeration: LinPEAS, Linux Exploit Suggester
- Reporting: Markdown editors, OpenVAS or other scanners' built-in report features

Industrial Cyber Security		Semester	6
Course Code	**BCYL657A**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	0:0:2:0	SEE Marks	50
Credits	01	Exam Hours	100
Examination type (SEE)	Practical		

Course objectives:

- To demonstrate network traffic analysis and intrusion detection.
- To understand security for ICS and PLC environments.
- To gain knowledge on configuration files for firewalls and Web systems.
- To conduct experiments for Incident Response Simulation and risk assessment.

Sl.NO	Experiments
NOTE: the experiments are to be carried out in a team of size 2 or 3.	
1	**Network Traffic Analysis in ICS/SCADA Systems** **Scenario:** A manufacturing plant experiences intermittent communication issues between its SCADA system and field devices. IT suspects abnormal traffic patterns are overwhelming the network. **Objective**: Use Wireshark to capture and analyze network traffic to detect anomalies such as unauthorized Modbus commands or excessive network scanning. **Tools** : Wireshark **Deliverables**: A detailed report of the traffic analysis, highlighting malicious or unusual traffic patterns and recommendations for mitigation.
2	**Configuring and Testing an Intrusion Detection System (IDS)** **Scenario**: An oil refinery has deployed an IDS in its control room but has not tested its effectiveness. Simulated attacks are needed to evaluate the IDS's detection capability. **Objective**: Configure Snort with custom rules to detect unauthorized login attempts, PLC command injections, or DoS attacks on the refinery's network. **Tools**: Snort **Deliverables**: A configured IDS, attack simulation results, and a performance evaluation report.
3	**Vulnerability Assessment of a Simulated ICS Network** **Scenario**: A power plant is transitioning to a new ICS network. The cybersecurity team must perform a vulnerability assessment before the network goes live. **Objective**: Scan the simulated ICS network for open ports, outdated software, and misconfigurations. **Tools**: Nmap, OpenVAS **Deliverables**: A vulnerability assessment report listing critical issues, potential exploitation risks, and suggested fixes.
4	**Securing a PLC Environment** **Scenario**: A water treatment facility reports unauthorized access to its PLCs, leading to erroneous water treatment settings. Students are tasked to secure the PLC environment. **Objective**: Simulate unauthorized PLC access, implement secure configurations, and monitor PLC traffic for anomalies. **Tools**: OpenPLC, Wireshark **Deliverables**: A secured PLC configuration and a log of identified unauthorized commands.
5	**Simulating Cyber Attacks on ICS and Designing Defenses**

	Scenario: An attacker compromises an engineering workstation and uses it to issue malicious commands to ICS devices. Students must simulate this attack and propose defenses. **Objective**: Perform simulated attacks such as PLC logic manipulation and denial-of-service, then implement measures like firewall rules or intrusion prevention systems. **Tools**: Metasploit Framework, Security Onion **Deliverables**: A report describing the attack, its impact, and the defense mechanisms implemented.
6	**Web Application Security for Industrial Systems** **Scenario**: The web-based interface of a chemical plant's ICS is suspected to have vulnerabilities that attackers could exploit to alter chemical mix ratios. **Objective**: Conduct a security assessment of the web interface for vulnerabilities like SQL injection, cross-site scripting, and improper authentication mechanisms. **Tools**: OWASP ZAP **Deliverables**: A vulnerability scan report with remediation recommendations for the ICS web application.
7	**Securing ICS Protocols and Communication Channels** **Scenario**: A logistics company faces unauthorized Modbus/TCP communication between its control system and conveyor belt motors, disrupting operations. **Objective**: Configure secure communication using encryption and analyze normal vs. malicious protocol traffic. **Tools**: OpenSSL, Wireshark **Deliverables**: Secured Modbus/TCP communication setup and a comparative analysis of traffic logs.
8	**Incident Response Simulation in an ICS Environment** **Scenario**: A simulated ransomware attack encrypts critical ICS files at a gas distribution station. Students act as the incident response team. **Objective**: Detect the ransomware, isolate affected systems, and recover operations using backup and monitoring tools. **Tools**: Security Onion, GRR **Deliverables**: An incident response report, including root cause analysis and recovery steps.
9	**Firewall and Access Control Configuration for ICS** **Scenario**: An unauthorized laptop connects to the ICS network at a steel factory and issues shutdown commands to operational systems. **Objective**: Implement access control policies and configure firewalls to block unauthorized devices and restrict communication to trusted sources. **Tools**: pfSense, ModSecurity **Deliverables**: Firewall and access control configuration files, along with a report on unauthorized device mitigation.
10	**Risk Assessment and Mitigation Planning for ICS** **Scenario**: A renewable energy plant wants to evaluate cybersecurity risks before connecting its wind turbines to the grid. **Objective**: Conduct a risk assessment considering hardware vulnerabilities, communication protocols, and environmental factors. Propose a mitigation plan. **Tools**: Custom scripts, risk assessment frameworks **Deliverables**: A comprehensive risk assessment report and a prioritized mitigation strategy.

Course outcomes (Course Skill Set):

At the end of the course the student will be able to:

- Experiment with network traffic analysis and intrusion detection.
- Demonstrate ICS and PLC environment security.
- Develop configuration files for firewall and Web systems.
- Experiment with risk assessment and incident response in ICS environment.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together

Continuous Internal Evaluation (CIE):

CIE marks for the practical course are **50 Marks**.

The split-up of CIE marks for record/ journal and test are in the ratio **60:40**.

- Each experiment is to be evaluated for conduction with an observation sheet and record write-up. Rubrics for the evaluation of the journal/write-up for hardware/software experiments are designed by the faculty who is handling the laboratory session and are made known to students at the beginning of the practical session.
- Record should contain all the specified experiments in the syllabus and each experiment write-up will be evaluated for 10 marks.
- Total marks scored by the students are scaled down to **30 marks** (60% of maximum marks).
- Weightage to be given for neatness and submission of record/write-up on time.
- Department shall conduct a test of 100 marks after the completion of all the experiments listed in the syllabus.
- In a test, test write-up, conduction of experiment, acceptable result, and procedural knowledge will carry a weightage of 60% and the rest 40% for viva-voce.
- The suitable rubrics can be designed to evaluate each student's performance and learning ability.
- The marks scored shall be scaled down to **20 marks** (40% of the maximum marks).

The Sum of scaled-down marks scored in the report write-up/journal and marks of a test is the total CIE marks scored by the student.

Semester End Evaluation (SEE):

- SEE marks for the practical course are 50 Marks.
- SEE shall be conducted jointly by the two examiners of the same institute, examiners are appointed by the Head of the Institute.
- The examination schedule and names of examiners are informed to the university before the conduction of the examination. These practical examinations are to be conducted between the schedule mentioned in the academic calendar of the University.

- All laboratory experiments are to be included for practical examination.
- (Rubrics) Breakup of marks and the instructions printed on the cover page of the answer script to be strictly adhered to by the examiners. **OR** based on the course requirement evaluation rubrics shall be decided jointly by examiners.
- Students can pick one question (experiment) from the questions lot prepared by the examiners jointly.
- Evaluation of test write-up/ conduction procedure and result/viva will be conducted jointly by examiners.

General rubrics suggested for SEE are mentioned here, writeup-20%, Conduction procedure and result in -60%, Viva-voce 20% of maximum marks. SEE for practical shall be evaluated for 100 marks and scored marks shall be scaled down to 50 marks (however, based on course type, rubrics shall be decided by the examiners)

Change of experiment is allowed only once and 15% of Marks allotted to the procedure part are to be made zero.

The minimum duration of SEE is 02 hours

Suggested Learning Resources:

Textbooks:

1. P. Ackerman, Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems. Packt Publishing, 2021.
2. T. Macaulay and B. Singer, Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press, 2012.

Reference Books:

1. C. Bodungen, B. Singer, A. Shbeeb, K. Wilhoit, and S. Hilt, Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. McGraw-Hill, 2017.
2. P. A. Craig Jr., Practical Industrial Cybersecurity: IT and OT Convergence. Wiley, 2021.
3. Ginter, SCADA Security: What's Broken and How to Fix It. Waterfall Security Solutions, 2016.

Generative AI		Semester	6
Course Code	**BAIL657C**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	0:0:1:0	SEE Marks	50
Credits	01	Exam Hours	100
Examination type (SEE)	Practical		

Course objectives:

- Understand the principles and concepts behind generative AI models
- Explain the knowledge gained to implement generative models using Prompt design frameworks.
- Apply various Generative AI applications for increasing productivity.
- Develop Large Language Model-based Apps.

Sl.NO	Experiments
1.	Explore pre-trained word vectors. Explore word relationships using vector arithmetic. Perform arithmetic operations and analyze results.
2.	Use dimensionality reduction (e.g., PCA or t-SNE) to visualize word embeddings for Q 1. Select 10 words from a specific domain (e.g., sports, technology) and visualize their embeddings. Analyze clusters and relationships. Generate contextually rich outputs using embeddings. Write a program to generate 5 semantically similar words for a given input.
3.	Train a custom Word2Vec model on a small dataset. Train embeddings on a domain-specific corpus (e.g., legal, medical) and analyze how embeddings capture domain-specific semantics.
4.	Use word embeddings to improve prompts for Generative AI model. Retrieve similar words using word embeddings. Use the similar words to enrich a GenAI prompt. Use the AI model to generate responses for the original and enriched prompts. Compare the outputs in terms of detail and relevance.
5.	Use word embeddings to create meaningful sentences for creative tasks. Retrieve similar words for a seed word. Create a sentence or story using these words as a starting point. Write a program that: Takes a seed word. Generates similar words. Constructs a short paragraph using these words.
6.	Use a pre-trained Hugging Face model to analyze sentiment in text. Assume a real-world application, Load the sentiment analysis pipeline. Analyze the sentiment by giving sentences to input.
7.	Summarize long texts using a pre-trained summarization model using Hugging face model. Load the summarization pipeline. Take a passage as input and obtain the summarized text.
8.	Install langchain, cohere (for key), langchain-community. Get the api key(By logging into Cohere and obtaining the cohere key). Load a text document from your google drive . Create a prompt template to display the output in a particular manner.
9.	Take the Institution name as input. Use Pydantic to define the schema for the desired output and create a custom output parser. Invoke the Chain and Fetch Results. Extract the below Institution related details from Wikipedia: **The founder of the Institution. When it was founded. The current branches in the institution . How many employees are working in it. A brief 4-line summary of the institution.**
10	Build a chatbot for the Indian Penal Code. We'll start by downloading the official Indian Penal Code document, and then we'll create a chatbot that can interact with it. Users will be able to ask questions about the Indian Penal Code and have a conversation with it.

Course outcomes (Course Skill Set):

At the end of the course the student will be able to:

- Develop the ability to explore and analyze word embeddings, perform vector arithmetic to investigate word relationships, visualize embeddings using dimensionality reduction techniques
- Apply prompt engineering skills to real-world scenarios, such as information retrieval, text generation.
- Utilize pre-trained Hugging Face models for real-world applications, including sentiment analysis and text summarization.
- Apply different architectures used in large language models, such as transformers, and understand their advantages and limitations.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together

Continuous Internal Evaluation (CIE):

CIE marks for the practical course are **50 Marks**.

The split-up of CIE marks for record/ journal and test are in the ratio **60:40**.

- Each experiment is to be evaluated for conduction with an observation sheet and record write-up. Rubrics for the evaluation of the journal/write-up for hardware/software experiments are designed by the faculty who is handling the laboratory session and are made known to students at the beginning of the practical session.
- Record should contain all the specified experiments in the syllabus and each experiment write-up will be evaluated for 10 marks.
- Total marks scored by the students are scaled down to **30 marks** (60% of maximum marks).
- Weightage to be given for neatness and submission of record/write-up on time.
- Department shall conduct a test of 100 marks after the completion of all the experiments listed in the syllabus.
- In a test, test write-up, conduction of experiment, acceptable result, and procedural knowledge will carry a weightage of 60% and the rest 40% for viva-voce.
- The suitable rubrics can be designed to evaluate each student's performance and learning ability.
- The marks scored shall be scaled down to **20 marks** (40% of the maximum marks).

The Sum of scaled-down marks scored in the report write-up/journal and marks of a test is the total CIE marks scored by the student.

Semester End Evaluation (SEE):

- SEE marks for the practical course are 50 Marks.
- SEE shall be conducted jointly by the two examiners of the same institute, examiners are appointed by the Head of the Institute.

- The examination schedule and names of examiners are informed to the university before the conduction of the examination. These practical examinations are to be conducted between the schedule mentioned in the academic calendar of the University.
- All laboratory experiments are to be included for practical examination.
- (Rubrics) Breakup of marks and the instructions printed on the cover page of the answer script to be strictly adhered to by the examiners. **OR** based on the course requirement evaluation rubrics shall be decided jointly by examiners.
- Students can pick one question (experiment) from the questions lot prepared by the examiners jointly.
- Evaluation of test write-up/ conduction procedure and result/viva will be conducted jointly by examiners.

General rubrics suggested for SEE are mentioned here, writeup-20%, Conduction procedure and result in -60%, Viva-voce 20% of maximum marks. SEE for practical shall be evaluated for 100 marks and scored marks shall be scaled down to 50 marks (however, based on course type, rubrics shall be decided by the examiners)

Change of experiment is allowed only once and 15% of Marks allotted to the procedure part are to be made zero.

The minimum duration of SEE is 02 hours

Suggested Learning Resources:

Books:

1. Modern Generative AI with ChatGPT and OpenAI Models: Leverage the Capabilities of OpenAI's LLM for Productivity and Innovation with GPT3 and GPT4, by Valentina Alto, Packt Publishing Ltd, 2023.
2. Generative AI for Cloud Solutions: Architect modern AI LLMs in secure, scalable, and ethical cloud environments, by Paul Singh, Anurag Karuparti ,Packt Publishing Ltd, 2024.

Web links and Video Lectures (e-Resources):

- https://www.w3schools.com/gen_ai/index.php
- https://youtu.be/eTPiL3DF27U
- https://youtu.be/je6AlVeGOV0
- https://youtu.be/RLVqsA8ns6k
- https://youtu.be/0SAKM7wiC-A
- https://youtu.be/28_9xMyrdjg
- https://youtu.be/8iuiz-c-EBw
- https://youtu.be/7oQ8VtEKcgE
- https://youtu.be/seXp0VWWZV0

DEVOPS		Semester	6
Course Code	**BCSL657D**	CIE Marks	50
Teaching Hours/Week (L:T:P: S)	0:0:2:0	SEE Marks	50
Credits	01	Exam Hours	100
Examination type (SEE)	Practical		

Course objectives:

- To introduce DevOps terminology, definition & concepts
- To understand the different Version control tools like Git, Mercurial
- To understand the concepts of Continuous Integration/ Continuous Testing/ Continuous Deployment)
- To understand Configuration management using Ansible
- Illustrate the benefits and drive the adoption of cloud-based Devops tools to solve real world problems

Sl.NO	Experiments
1	**Introduction to Maven and Gradle:** Overview of Build Automation Tools, Key Differences Between Maven and Gradle, Installation and Setup
2	**Working with Maven:** Creating a Maven Project, Understanding the POM File, Dependency Management and Plugins
3	**Working with Gradle:** Setting Up a Gradle Project, Understanding Build Scripts (Groovy and Kotlin DSL), Dependency Management and Task Automation
4	**Practical Exercise:** Build and Run a Java Application with Maven**,** Migrate the Same Application to Gradle
5	**Introduction to Jenkins:** What is Jenkins?, Installing Jenkins on Local or Cloud Environment, Configuring Jenkins for First Use
6	**Continuous Integration with Jenkins:** Setting Up a CI Pipeline**,** Integrating Jenkins with Maven/Gradle**,** Running Automated Builds and Tests
7	**Configuration Management with Ansible:** Basics of Ansible: Inventory, Playbooks, and Modules, Automating Server Configurations with Playbooks, Hands-On: Writing and Running a Basic Playbook
8	**Practical Exercise:** Set Up a Jenkins CI Pipeline for a Maven Project, Use Ansible to Deploy Artifacts Generated by Jenkins
9	**Introduction to Azure DevOps:** Overview of Azure DevOps Services, Setting Up an Azure DevOps Account and Project
10	**Creating Build Pipelines:** Building a Maven/Gradle Project with Azure Pipelines, Integrating Code Repositories (e.g., GitHub, Azure Repos), Running Unit Tests and Generating Reports
11	**Creating Release Pipelines:** Deploying Applications to Azure App Services, Managing Secrets and Configuration with Azure Key Vault, Hands-On: Continuous Deployment with Azure Pipelines
12	**Practical Exercise and Wrap-Up:** Build and Deploy a Complete DevOps Pipeline, Discussion on Best Practices and Q&A

Course outcomes (Course Skill Set):

At the end of the course the student will be able to:

- Demonstrate different actions performed through Version control tools like Git.
- Perform Continuous Integration and Continuous Testing and Continuous Deployment using Jenkins by building and automating test cases using Maven & Gradle.
- Experiment with configuration management using Ansible.
- Demonstrate Cloud-based DevOps tools using Azure DevOps.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 40% of the maximum marks (20 marks out of 50) and for the SEE minimum passing mark is 35% of the maximum marks (18 out of 50 marks). A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures a minimum of 40% (40 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together

Continuous Internal Evaluation (CIE):

CIE marks for the practical course are **50 Marks**.

The split-up of CIE marks for record/ journal and test are in the ratio **60:40**.

- Each experiment is to be evaluated for conduction with an observation sheet and record write-up. Rubrics for the evaluation of the journal/write-up for hardware/software experiments are designed by the faculty who is handling the laboratory session and are made known to students at the beginning of the practical session.
- Record should contain all the specified experiments in the syllabus and each experiment write-up will be evaluated for 10 marks.
- Total marks scored by the students are scaled down to **30 marks** (60% of maximum marks).
- Weightage to be given for neatness and submission of record/write-up on time.
- Department shall conduct a test of 100 marks after the completion of all the experiments listed in the syllabus.
- In a test, test write-up, conduction of experiment, acceptable result, and procedural knowledge will carry a weightage of 60% and the rest 40% for viva-voce.
- The suitable rubrics can be designed to evaluate each student's performance and learning ability.
- The marks scored shall be scaled down to **20 marks** (40% of the maximum marks).

The Sum of scaled-down marks scored in the report write-up/journal and marks of a test is the total CIE marks scored by the student.

Semester End Evaluation (SEE):

- SEE marks for the practical course are 50 Marks.
- SEE shall be conducted jointly by the two examiners of the same institute, examiners are appointed by the Head of the Institute.
- The examination schedule and names of examiners are informed to the university before the conduction of the examination. These practical examinations are to be conducted between the schedule mentioned in the academic calendar of the University.
- All laboratory experiments are to be included for practical examination.
- (Rubrics) Breakup of marks and the instructions printed on the cover page of the answer script to be strictly adhered to by the examiners. **OR** based on the course requirement evaluation rubrics shall be decided jointly by examiners.

- Students can pick one question (experiment) from the questions lot prepared by the examiners jointly.
- Evaluation of test write-up/ conduction procedure and result/viva will be conducted jointly by examiners.

General rubrics suggested for SEE are mentioned here, writeup-20%, Conduction procedure and result in -60%, Viva-voce 20% of maximum marks. SEE for practical shall be evaluated for 100 marks and scored marks shall be scaled down to 50 marks (however, based on course type, rubrics shall be decided by the examiners)

Change of experiment is allowed only once and 15% of Marks allotted to the procedure part are to be made zero.

The minimum duration of SEE is 02 hours

Suggested Learning Resources:

- https://www.geeksforgeeks.org/devops-tutorial/
- https://www.javatpoint.com/devops
- https://www.youtube.com/watch?v=2N-59wUIPVI
- https://www.youtube.com/watch?v=87ZqwoFeO88